TOP SECRET

DF 116-Y

40/49/TOPSEC/AS-14-TICOM

FLICKE: The Decipherment of the Fellers Messages

1. The attached is an Army Security Agency translation of a paper written by Wilhelm Flicke, former chief evaluator and the officially designated historian of the Signal Intelligence Agency of the Supreme Command, German Armed Forces.

2. The present paper, German title "Die Entzifferung der [illegible]," treats of the technical side of the Fellers case. The intelligence value of these message has already been discussed in the book "The War Secrets in the Aether."

23 May 1949
Translated: RWP
Distribution: Normal

30 copies: Copy No.____

13 pages.

The Decipherment of the Fellers Messages

Rarely does a throw for great stakes win, but when it does the laborious effort of many years has not been in vain. One of the peculiar things about the art and science of cryptanalysis is that one can never predict in advance whether there will be success. Often it is extremely depressing to sit before thousands and thousands of enciphered messages, to have to arrange and log them by systems, categories, and other characteristics and still not be able to raise the veil of secrecy a single time for even a few minutes.

If we consider how much expenditure of labor and money is required simply to assure the interception, with as few gaps as possible, of all the messages which a country of the size of the U.S.A. sends out into the aether daily, then it sometimes seems doubtful to every serious worker and specialist whether such an employment of workers is justified at times when every single man is needed.

If it is once possible to score one slight advance, however, it is rare that another proves impossible. The scientific research man feels some satisfaction, his collaborators - who have often worked for months or even for years with monotonous, dead letters or digits, compiled statistics, drawn curves, and made computations - they receive a new incentive.

When from the lifeless numbers and symbols single words and sentences develop, which in the beginning still look awkward and without connection and present a remarkable puzzle, it is still by no means clear whether the information is useful at all. It may be that these messages contain merely the transfer of combat engineer Smith or of grenadier Miller and report how much baggage he is taking along and whether he is going on a mission or returning from leave. No doubt these reports are without interest for the high command and yet a harmless message may become a treasure trove for further investigation.

Sometimes - but only rarely - fortune is especially gracious and then a successful throw comes at the right moment.

The German intercept and cryptanalytic service worked in collaboration with several countries. Mention of this fact has been made in several previous reports. It was mainly with Italy, Hungary, and Finland that a close cooperation existed. The cooperation of these "sister offices" in the leagued countries was not always esteemed very highly. Some worked honestly, but without proper means and proper leadership, to accomplish something worth while; others accomplished marvelous things and sometimes put the German cryptanalytic service to shame.

Those less successful in the scientific work often possessed other good qualities. So it was in the late summer of 1941 when one day at the Tirpitzufer in Berlin, where the central office of the German cryptanalytic service was located, a whole package of highly important material was laid on the table. The messenger smiled in friendly fashion and gave no response to questions as to "how" and "from where," but did add: "We've had luck".

The type of material, in particular the completeness of the codes, betrayed, however, that they had not been put together by years of detailed work. Paper and print showed that the photographic lens combined with the slyness and cunning of its owner could do the job more quickly than the scientific worker.

The goal, however, has not always been reached when a code is at hand. The further development and refinement of cryptographic methods has led to the use of additional security measures in order to prevent unauthorized reading, even in case the code falls into the hands of the enemy.

The favorite American system was encipherment by means of substitution tables. These have to be as complicated as possible, - the security is so much greater. On the other hand, they must not be too complicated to use so that the authorized code clerk can make use of them without making mistakes. When the process of encipherment makes too great demands on the cryptographic personnel, sources of error easily result. These are apt to delay the transmission of information because questions have to be sent back. In many cases the messages even have to be repeated. The content must remain the same but the form of the message is to be changed, so the

instructions say.

If the authorized code clerk does not exercise the necessary precautions, a weak point results and hence an opportunity for the enemy to break into the system.

Practical work during the war showed that the American cryptographic personnel was often guilty of such carelessness and so facilitated the work of the German cryptanalytic service; sometimes this was the only thing which made success possible.

It must be stated, however, that the discipline of the Americans improved materially in the last two years of the war and that breaches of discipline were observed more rarely.

For each code a limited period of validity is intended. Any frequent change is out of the question because the production of such an extensive work calls for very much time and expense. Difficulties of transportation and the risk of theft, even in a courier's baggage, on the way across enemy territory or across neutral states also come into account.

It often happened that individual offices were not able to read the enciphered messages because they were not in possession of the valid means of enciphering and deciphering. Although the receipt of new cipher material had to be reported immediately to the Department of State or the War Department and, consequently, Washington must be informed, such mistakes were made there frequently. Then repetitions were necessary in a code, or according to some other cryptographic system. If these were not done carefully, i.e., by clever alterations of the text, they yielded welcome points of attack for the German cryptanalytic service.

On the other hand, the German cryptanalytic service in this way often came into the possession of reports some days before the American offices for which they were intended but by which they could not be read.

Less important errors in encipherment were often recognized by the German cryptanalytic service so that even such messages could be deciphered with relatively little effort while the clerk in Ankara or Teneriffe had to radio to Washington one appeal for help after the other.

If the frequent replacement of a code or some other cryptographic system does not appear advisable, there is no objection if an encipherment is changed at relatively short intervals of time. This practice was also employed in the American systems and was refined during the course of the war by introducing changes in the composition of substitution tables and shortening the period of their validity. In this way the solution of cryptograms became a struggle against time. Naturally, messages which are solved late have only a limited value.

The diplomatic cryptographic systems of the State Department and the systems of the Military Attachees of the War Department had a relatively great similarity to one another; obviously they had been designed by a central office. Similar systems were also common in the Army and in the Navy.

In solving the Military Attache system in 1941 and 1942 the German cryptanalytic service was aided by experience derived from the solution of diplomatic systems, i. e., the cryptograms of the State Department. And these in turn could later be used to solve other systems in the diplomatic field.

The two most important Military Attache systems, which were employed in 1940 and 1941 and on into the summer of 1942, were the "Intelligence Code" and the "Confidential Code." As far as the significance of the content was concerned, the former far out-ranked the later. The code was a five-letter code (consonant, vowel, consonant, vowel, consonant) and not very extensive (some 3000 groups). The fifth element of a group could always be computed by means of a table; hence, errors due to imperfect reception could quickly be located and eradicated provided only a falsely copied letter was involved.

The code was not alphabetic, i. e., there was no alphabetic arrangement of the plain text opposite an alphabetic arrangement of a cipher group. The distribution of the letters within the five elements of the cipher groups was unsystematic so that no point of attack was given in this way.

With the "Intelligence Code" ten substitution tables were used, which, taken two and two, were always inverse to one another. Consonants were replaced by consonants and vowels by vowels; each table contained different substitution letters for a total of four groups, which were enciphered in normal sequence after the manner of a polyalphabetic substitution.

The use of the first substitution table employed in the message was shown by the "Cipher Indicator," which was placed behind the date group and sent in clear.

Then encipherment with this table continued in the manner just described taking four groups at a time, i. e., in phases, until a new "Cipher Indicator" appeared which announced the use of a new substitution table.

The use of the fourth group in a phase, often with regular intervals, facilitated the work of decipherment for the German cryptanalytic service.

The change of substitution tables resulted on the average after five to six phases [cycles]. A conscientious code clerk changed more frequently and saw to it that the intervals were as irregular as possible.

The weakness of any code, even when there are ever so many variants for frequent plain-text words or combinations, consists in the danger that the words occurring most frequently will be reflected in the cipher groups. It is a well known and a psychologically explicable fact that a few groups which are easily committed to memory will be given a preference. The encoder wants to save time and writes down from memory the familiar groups without looking them up in the code book.

In a code which is refined by a system of cleverly conceived substitution tables and hence is rendered far more complicated, the number of repetitions appearing in the cipher text - so-called "parallel passages" - is materially less. To achieve an entry the unauthorized decipherer must have many times as much traffic as would normally be the case. The preliminary statistical work increases correspondingly in volume and becomes more difficult and time consuming.

Nevertheless, even when ten different substitution tables are employed, it is possible to count on the occurrence of parallel passages (called "crocodiles" in the cryptographic section) which are useful and important for solving the cryptogram.

The likelihood is greatest when proper names occur. In a code of medium extent these are not represented by special cipher groups and must therefore be spelled out or at least broken up into groups of letters or syllables, if there are such in the code. The name "Rockefeller," for instance might be reproduced as follows:

ROCK - E - FELL - ER;

in other words, four plain-text words equal to four cipher groups. If the same name occurs again, perhaps by accident in the same message and even in the same phase and enciphered by the same substitution table, then we get the so-called "parallel passage" in the cipher text.

The same phenomenon occurs when names or designations of offices, institutions, ships, weapons, types of airplanes, and the like are involved which embrace several cipher groups.

The creator of the code had also forseen this weakness and introduced the so-called "Repeater," i. e., repeater groups. Such a group, placed after a word, signifies that in case of a repetition the whole series of cipher groups is not to appear again but only a single group which then automatically represents the entire word or the entire combination of words.

The repeater groups ("Repeaters") were also represented by several code groups (variants) so as to avoid too frequent occurrence. The length of the repetitions, i. e., the number of cipher groups, was shown by special repeater-group-families.

These measures not only contributed to the security of the cryptographic system but also at the same time reduced the length of the telegram or the radiogram.

In practical work, however, there is a type of repetitions which even a clever and experienced compiler of codes can hardly calculate and thus eliminate: these are the stereotyped expressions which occur over and over

again because they are practically unavoidable. They constitute the greatest weakness in the use of any code.

The cryptanalyst, however, watches with Argus eyes every suspicious constellation: practically every break into a code is due to them. Patience and watchfulness are the supreme rule in the intercept and cryptanalytic service. Nowhere else does human inadequacy reveal itself as it does here. It is always a question of waiting for the mistake that the enemy will make some day; and he will make it some day with absolute certainty.

It is true that the American Military Attache systems took this dangerous fact into account more and more as years went on; however, the camouflage tactics were not perfect enough to prevent the German cryptanalytic service from making use of this chance.

The messages enciphered with the "Intelligence Code" initially carried a statement of the originator and recipient at the message beginning, practically without a thought; frequently these involved seven or more cipher groups.

How did these addresses and signatures become known? -All you could tell by looking at the enciphered messages was that the same names might be involved, nothing more.

One must bear in mind that for cryptanalytic work a many-sided store of information has to serve as a base. Harmless plain-text messages or newspaper reports may give the most valuable hints. A well-managed archive, equipped in the most up-to-date fashion, renders invaluable service. Here are recorded with painstaking exactitude, and in a way which makes it possible to find them at a moment's notice, the names of all political and military personalities, as they become known; designations of offices, ships, weapons; data regarding treaties and agreements made; negotiations projected; political events; parliamentary debates; utterances of distinguished politicians; changes in cabinets or in military commands; accidents; special events; etc. It must be possible to answer at once every question of the cryptanalyst regarding anything which may have happened in any connection.

Of course, in spite of excellent data it is always up to the cryptanalyst to have the right inspiration at the right point, to develop a break-in logically, and not to deviate from his course, even though this sometimes may prove deceptive.

Not every well-founded assumption means a break-in; hard work is required to find final confirmation and prove the correctness of an hypothesis, or to reject it again and seek a new one. Often the cryptanalyst gets on the wrong track in spite of the correct assumption and is inclined to drop his plan if confirmation cannot be secured.

All these happened in connection with the "Intelligence Code," too. Above all else a good knowledge of the content of Military Attache traffic formed an important prerequisite for solution of the cryptographic system. In this connection there was excellent proof of the validity of the thoroughness with which this traffic was monitored at the Lauf intercept station, where the primary assignment was copying this traffic. The system of reception control used there gave assurance that the traffic was picked up virtually without gaps.

The labors which led to the solution of the first set of substitution tables occupied several months. In the spring of 1942 it was accomplished. Of course, it had been possible earlier to read a considerable portion of the messages, even though not in entirety. The telegrams read were somewhat old, to be sure, but their content was still of real value.

The most important traffic was the Cairo-Washington link. The American Military Attache, Fellers, had good information which he got from British Headquarters in Egypt. To the great delight of the German cryptanalytic service he was extraordinarily talkative. By this trait he did the German decoders a two-fold favor. In the first place, the material they had to work on became so abundant that the solution of the cryptographic systems was achieved much more quickly; in the second place, he supplied the German High Command with excellent intelligence material; no better and more dependable information could have been secured through agents or other sources. Moreover, it was probably absolutely true because the Military Attache was giving his War Department, without any adornment or propagandistic intent, a sober picture of the situation on

the enemy side and an equally sober picture of the situation on the German side.

After the first set of substitution tables was solved, the ice was broken. The first completely deciphered messages had been translated and passed on. The interest of the German military command was extraordinarily great and grew from day to day. The only question, which was put regularly along with laudatory commendation, was:

"When are we going to get the latest reports?"

The work was carried on feverishly in several shifts but a solution cannot be forced in this manner. It grips all those participating in the work, like an exciting novel, the end of which you want to reach quickly. But just as you have to work your way through a big fat book, it was necessary to mount from one stage to the next in order after occasional tarryings and short detours to arrive at last on the summit of the mountain.

As everywhere, practice and familiarity with the code played an essential role here. The dead letters of a cipher group take on life, become people, tanks, infantry regiments, and friends or foes. The smaller ones among them, however, the prepositions "from" and "for," are of particular interest; they attend each person and each thing. The proper names become especially dear when they are as long as possible and show characteristic qualities in their cipher groups, e. g., when they extend over five or more cipher groups and, when in phase, have like components in the groups such as:

CIMEG and BOMAG.

These cannot be disguised even by encipherment with substitution tables and become for the cryptanalyst precious things to be sought out. Often, even in the case of the Fellers messages, they guided the German cryptanalytic service to the proper path.

The Cairo traffic was especially pleasing to the German cryptanalysts in this respect. Every week the ships entering and leaving the Suez canal were reported from Alexandria to Washington. These reports were doubtless interesting and important for the German Navy and the German Air Force. And yet they were far more important for the German cryptanalysts, for they

were probably the weakest spot in the whole cryptographic system or - to state it more precisely - in the use of the system. With absolute certainty those shipping reports appeared at the end of each week, rarely differing by a day. They contained almost the same wording or differed so slightly that a practiced eye - and a good cryptanalyst must have one - could quickly fill in the remaining blank cells of the "cross-word puzzle."

It may be mentioned in passing that the incoming and outgoing ships were often reported not merely once but two or even three times. With almost 100 percent certainty the incoming ships appeared the next weekend as outgoing. If they stayed longer than a week in the harbor of Alexandria, the German cryptanalytic service was prone to mark them down for the following Sunday; consequently, they knew the ships' names with which they would have to deal; and thus the delay of a ship in the harbor of Alexandria repeatedly helped to clear up new cryptographic connections and to defeat the cryptographic system more and more.

These reports were generally not long and therefore could readily be picked out among the five to ten other messages received. An occasional wrong guess delayed success but did not check the work in any essential way.

It would take us too far afield to explain here the details of the methodic procedure; we shall only say that the utmost exactitude and the most precise graduation of a new system according to its probability were the most significant conditions for preventing a laboriously constructed hypothesis from finally crumbling into ruin.

Errors of the operator or of the intercept operator often played a decisive role. If, for example, a cipher group had been omitted, then the picture changed radically and led to misinterpretations. If the operator who received the message or the clerk who copied it off the tape carelessly left out a group, read it off incorrectly, or merely confused single letters, then it was all up with the correct interpretation. There were also other sources of error: Atmospheric or technical disturbances prevented good reception, even if the operator was ever so

capable. How often it happened that precisely the most important messages, which one had been waiting for longingly, arrived horribly garbled. Although time was pressing, nevertheless it was necessary again and again to exercise the greatest patience.

Experience and routine, in conjunction with an exactly functioning intellect and a lucky hand, always came to the aid of the cryptanalyst in the long run. If the first substitution table required perhaps a week for complete solution, the same work could be accomplished in a third or a quarter of the time when the conditions were favorable. In any event, the shipping messages from Alexandria could not have been arranged more thoughtfully or better for the success of the German cryptanalytic work. At the time when the German Afrika Korps was preparing for the last great offensive, which ultimately got to El Alamein, the German cryptanalytic service was able to supply Rommel with information of the very highest value. All the cryptanalysts who had worked on the solution of this system regarded this success as a reward for the months of labor and for their persistence during the alternate ups and downs of the initial successes. The solution of the substitution tables had to be achieved with the utmost speed if the reports were to be of real value.

In the weeks preceding Whitsuntide 1942 it became clear that a unique opportunity had been given the German cryptanalytic service. The technical organization had become splendidly adjusted. The best intercept operators were sitting at their instruments in Leaf near Nuernberg and in Treuenbrietzen near Berlin; a select group working day and night shifts had been assigned primarily to intercept the Cairo traffic. All frequencies on which this traffic was sent were known so that one need hardly reckon with the loss of messages.

As a check, all messages were intercepted twice if additional equipment was available. As soon as an operator recognized the familiar address of the telegram, the cryptanalytic section in Berlin was notified. The number of groups could be learned from the message heading. Not infrequently actual tape messages were transmitted which were forwarded in single parts by special messenger to the cryptanalytic section. Thus it happened that

before the last part had been copied off the receiver tape the first had already progressed to a point where rough outlines of the content could already be recognized.

Each message was "prepared" rationally so that several analysts could work on it simultaneously. It was essential to recognize the starting point for new encipherment tables; then the rest came automatically. The fragments gave a kaleidoscopic picture of sentences, frequently of only part of sentences or single words, among which repeater groups and the like were scattered. Ultimately, however, it all pieced together like a mosaic to give a complete picture. Groups which had been wrongly intercepted or garbled in sending and made no sense were checked and figured out. Rarely was a gap left open. The translator dictated the completed messages to the machine at once; in an hour or less a report could start on its way to Africa through the same aether through which it had come.

In the decisive days when the German Afrika Korps was beginning its last drive to the East, which seemingly promised to be successful, the German cryptanalytic service was able for weeks to lay before Rommel the same very realistic reports just as quickly and perhaps even more quickly than they were transmitted to the Chief of the American General Staff in Washington by his Military Attache, Colonel Fellers, in Cairo. Messages containing errors due to the code clerk in Cairo could be read by the German analysts after the errors had been recognized. By the time that Washington's queries and requests for a repetition were on their way through the aether, the deciphered telegram was already in Rommel's possession.

It gave the German cryptanalysts special delight when they could outstrip the code clerk in Washington, who worked mechanically. Sometimes they would have been glad to help him out a little.

Nevertheless, among the German cryptanalysts there was always a certain concern. When would X-Day come, the day when the old set of substitution tables would be replaced? That it would come soon after the great offensive was clear; and yet the German decoders wondered at the American lack of concern which did not cause it to come much sooner.

Faultily enciphered telegrams were often looked upon as the signal, but in every case they turned out to be merely a mistake.

The German cryptanalytic organization was as well prepared as possible for the day of the change. Girls who worked swiftly and cleverly on statistics sat ready to enter in fat volumes the hundreds of apparently lifeless cipher groups, to arrange them systematically, and to assign each group to the proper square. Erroneously copied groups could easily do more harm than good and correcting was more difficult than entering.

The first parallel passage laid the foundation for the new structure. Characteristic weaknesses, for which the authorized encoders or Mr. Fellers were personally responsible, contributed their share to get the new set of substitution tables going in the shortest possible time even in these decisive weeks. The previously mentioned shipping reports from Port Said and the Suez Canal proved loyal helpers at this time, too. The folders which had meanwhile become greatly swollen grew thinner. "Solved subsequently" was noted on the deciphered radiograms. They went out along with those which were up-to-date and of prime priority.

A layman might have been surprised at this mixture of dates and hit upon the idea that some office had been napping for a time. The sober notation "Solved subsequently" was intended to give an explanation and tell those who did not understand why the most recent reports had failed to come, that reports of this kind could not be produced by machine methods but called for the most strenuous mental toil.

After the solution of the new substitution tables was again well underway, reports could be deciphered which had the same high military value as before until that celebrated compromise through a radio play on the German broadcasting station occurred, whereupon the entire code was replaced.

Details regarding the deciphered telegrams will be given in a later report.